United States Army Signal Center, Fort Gordon, Georgia
Leader College of Information Technology

The MSRT to RAU Protocol Reference Model

Functional Area 24 Telecommunications Systems Engineer Course Class 05-01

Lou L. Burton III, Dirk K. Brock, Matthew W. Dunlop, and Brian M. Tung

lou.burton@us.army.mil dirk.brock@us.army.mil matthew.dunlop@us.army.mil brian.tung@us.army.mil

24 January 2002

Table of Contents

The MSRT to RAU Protocol Reference Model

Lou L. Burton III, Dirk K. Brock, Matthew W. Dunlop, Brian M. Tung

lou.burton@us.army.mil dirk.brock@us.army.mil
matthew.dunlop@us.army.mil brian.tung@us.army.mil

1. Introduction

Integration of commercial technology into military communications systems serves to reduce the cost of improved capability while minimizing interoperability difficulties between service components or allied forces. Historically, the military has been a principle driver of information system and telecommunication system development. Today, however, private sector demands for reliability, security, and flexibility have also led to vast improvements in readily available technology. Better understanding of industry telecommunications models will assist military communicators in making informed decisions about the appropriate selection of commercial-off-the-shelf (COTS) technology to replace or enhance existing systems and subsystems. The following investigation of the Army's legacy wireless telephone system demonstrates that industry models can be effectively applied to proprietary systems. Previous work[a] in this area [1] has proposed that the instruction of tactical communications systems to Army signal officers is significantly improved when based upon industry models. Delving into the operations of the wireless telephone subsystem of Mobile Subscriber Equipment (MSE) leads to a better understanding of MSE in terms of industry models and establishes a basis for evaluating strategies for commercial technology integration.

2. Background

Designed and fielded during the Cold War, Mobile Subscriber Equipment (MSE) is a common-user, switched, digital communication system of linked switching nodes. Together, these mobile switching and access nodes form a communications grid that provides the force with an area common-user system (ACUS) capable of passing both voice and data. Node Center (NC) Switches (NCSs) provide trunk (tandem) switching, while Small Extension Node (SEN) switches Large Extension Node (LEN) switches and Radio Access Units (RAUs) provide local access to stationary and mobile subscribers. Cable, line-of-site radios, and satellite terminals provide inter-nodal connectivity. Advances in telecommunications technology have led to the integration of better data systems into the MSE architecture. This evolutionary process has led to the Army vision of a future Warfighter Information Network—Tactical (WIN-T), which promises greater reliance on COTS technology and abandons many of the vendor specific solutions of MSE. Never the less, many components of the legacy MSE system will remain in the Army inventory until 2010. One such item is the Mobile Subscriber Radio-telephone Terminal (MSRT), an end user system that has no identified or proposed replacement in the new architecture.

[a] The Mobile Subscriber Equipment (MSE) Telecommunications Functional Model developed by students in a previous Telecommunications Systems Engineer Course (TSEC) class models the MSE network as a whole. The protocol reference model proposed in this paper is much narrower in focus, concentrating only on the wireless components required for MSRT operations.

2.1. Overview of MSRT-RAU Operations

The MSRT provides end users access to the MSE network through what can best be described as a "tethered wireless" arrangement [2]. True cellular systems allow connections to be passed from one tower to the next seamlessly. These "handovers" allow wireless devices to move from one cell to another without breaking connections. MSRTs access the MSE switched telephone network through Radio Access Units (AN/TRC-191 / RAUs). Placed calls remain in effect for as long as the caller remains within the signal footprint of the RAU. Once the signal is lost, the user must redial the MSRT and access the network through another RAU. This tethered mobility is much easier, and cheaper, to implement than full mobility.

The MSRT consists of both telephone and radio components as illustrated in Figure 1. The Digital Secure Voice Terminal (KY68/DSVT) is a cryptographic four-wire[b] telephone built for field use. The RT-1539 Mobile Subscriber Radio Terminal operates full duplex in the VHF frequency range (30-88 MHz). Each RAU contains eight RT-1539s used to support up to eight wireless subscribers at a nominal range of 15 km [3]. The RAU multiplexes the signals from the eight radios and sends them to a node center switch through a UHF radio or coaxial cable connection. Several components necessary to the operation of the MSRT and RAU, indicated by gray boxes, serve supporting roles to the principle functions, but are not necessary for model development.

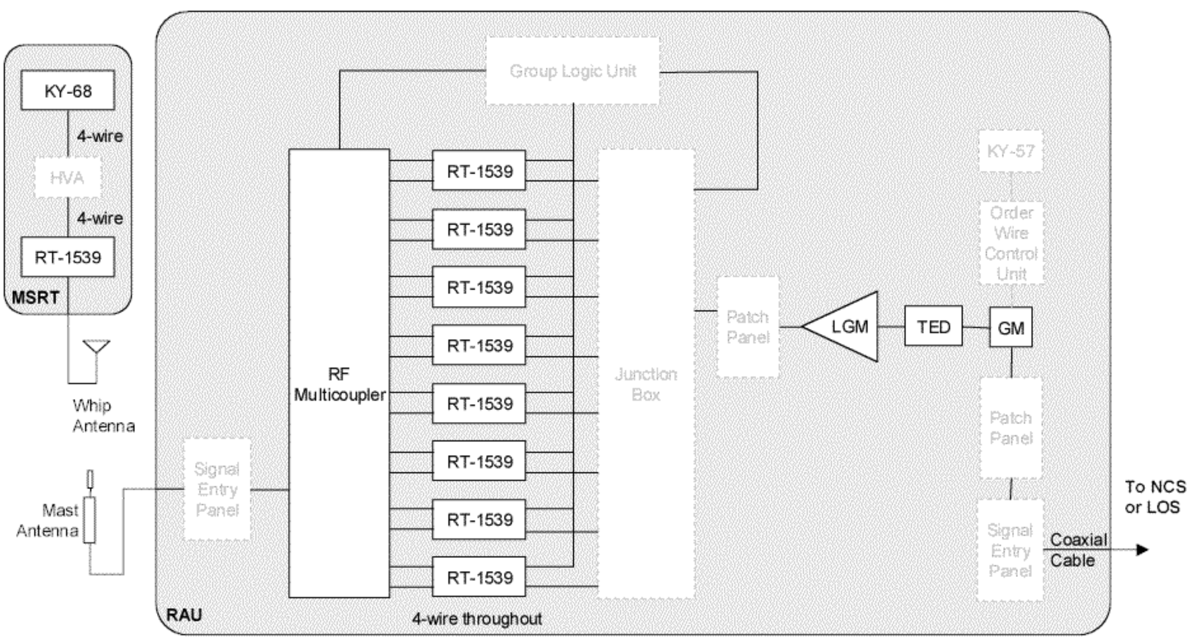


Figure 1. Principle Components of the MSRT and RAU

[b]The term "four-wire" used throughout the document refers to a logical four-wire circuit, which is full-duplex. The actual connections between each device comply with standard military specifications.

2.2. Open Standards in the Military Information Space

Since the approval of the original MSE Operational Capability document in 1984, MSE has undergone a number of enhancements to include the addition of packet switching capability and integration with data radios. Further enhancements are currently being defined under the proposed WIN-T architecture. The WIN-T architecture recognizes the continuing convergence of communications and computing and seeks to use more COTS technology to pass both voice and data in a highly mobile environment where troops may be widely dispersed.

The WIN-T Project Manager (PM) retains responsibility for the improvement or replacement of all major components of the MSE system, but the Army's Communications Electronics Command (CECOM) retains responsibility for the MSRT and RAU [4]. This assignment of responsibilities suggests that the PM would prefer to look at new wireless technologies rather than develop a wireless solution that specifically replaces the MSRT/RAU arrangement. The Fort Gordon Battle Command Battle Lab (BCBL-FG) has already demonstrated the use of COTS wireless communications systems surrounding Brigade Subscriber Nodes (BSNs)[c] and several vendors at the November 2001 Signal Symposium demonstrated several technologies to provide cellular capabilities to military units over multiple cellular networks. With this emphasis on moving to new wireless solutions, some might suggest that there is little need to look at a legacy system. There are three good reasons for doing so.

First, MSRTs greatly extend the range of the switched network. RAUs provide access to tactical users in the battalion areas, while switches tend to serve users at brigade and above. Demonstrations have shown that cellular telephones can service the immediate area of a brigade subscriber node (BSN) switch, but have not yet addressed how service will be provided forward of the brigades. Understanding the MSRT-RAU operations will help to determine whether the existing configuration could be modified to accommodate the same cellular devices accommodated by the BSN.

Second, despite the many advantages of adopting COTS technologies, there are often reasons for developing military specific solutions. One RAND researcher has noted that military-unique systems requirements "tend to drive the design of military communications systems that are markedly different from commercial systems." These requirements include low probability of detection (LPD), resistance to jamming, precedence and perishability, electromagnetic compatibility, interoperability with legacy systems, and security [5]. Revisiting RAU operations may provide insights into the design of future systems that continue to meet these objectives.

Third, as the Army signal architecture adapts more data-based solutions, communications personnel will become accustomed to thinking of telecommunications systems in terms of the OSI and TCP/IP models. Developing an appropriate model for teaching this legacy system will assist communications personnel to understand MSRT-RAU operations in the language of current technology.

3. Goal

To develop an MSRT to RAU Protocol Reference Model that describes the control, user, security, and management functions supporting wireless MSE communications. To build upon

---

[c] Under WIN-T, BSN switches replace the SEN switches used in the current architecture, while adding improved switching and routing features. Demonstrations have already shown the use of BSNs as strategic-tactical entry point (STEP) sites, providers of wireless local area networks, and access points for cellular systems.

the seven-layer ITU-T X.200 Open Systems Interconnection (OSI) Model, the ITU-T I.320 ISDN Protocol Reference Model, and the Individual End System Component Functionality Model, demonstrating the effectiveness of such models for instruction, and building a foundation for assessing points of integration for COTS technology into the MSRT-RAU operation.

4. Scope

The MSRT to RAU Protocol Reference Model focuses on MSRT-RAU user protocols, control protocols, security protocols, and management protocols. The MSRT to RAU Protocol Reference Model is based upon the industry standard, seven-layer OSI Reference Model, concentrating on Layer 0—Physical Media, Layer 1—Physical Interfaces, Layer 2—Data Link, and Layer 3—Network. It views the Transport, Session, Presentation, and Application layers (Layers 4-7) collectively as "Higher Layer Protocols." In order to show the interactions between components, the model draws upon the ITU-T ISDN Protocol Reference Model (Figure 2) and adds a Security Protocol Block. Finally, in order to understand interactions between components, it draws upon the Individual End System Component Functionality Model, as introduced in the next section. The final Protocol Reference Model does not follow the OSI layers precisely, but, by obeying the same rigorous principles and thought processes, results in a model that provides a solid foundation for further study.

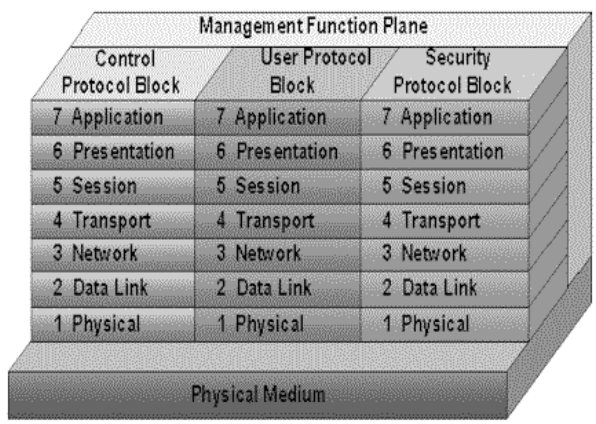


Figure 2. Modified I.320 ISDN Protocol Reference Model with Security Block Added

5. The Control Protocol Plane

Control plane protocols transfer information in order to set up and break down network connections, control multiple network connections, control the use of already established network connections, and provide supplementary services [6]. Control has interaction with components in all of the other functional groups of termination and access, transport, and switching components. Control signals are signals exchanged between subscribers and switches or between switches to request or control the services provided [7].

5.1. Overview

Within MSE, control interactions are required to complete automatic mobile subscriber affiliation, automatic affiliation transfer of mobile subscribers, disaffiliation, automatic affiliation, calls to or from mobile subscribers, transfer of calls to mobile subscribers, progressive and preprogrammed conference, and other general features provided to mobile subscribers. As discussed in the management section, affiliation, or address registration, is a management function. The process to set up the passage of management information, however, is a control function. The control messages passed to complete the essential functions of affiliation and call establishment are shown in Figure 3.

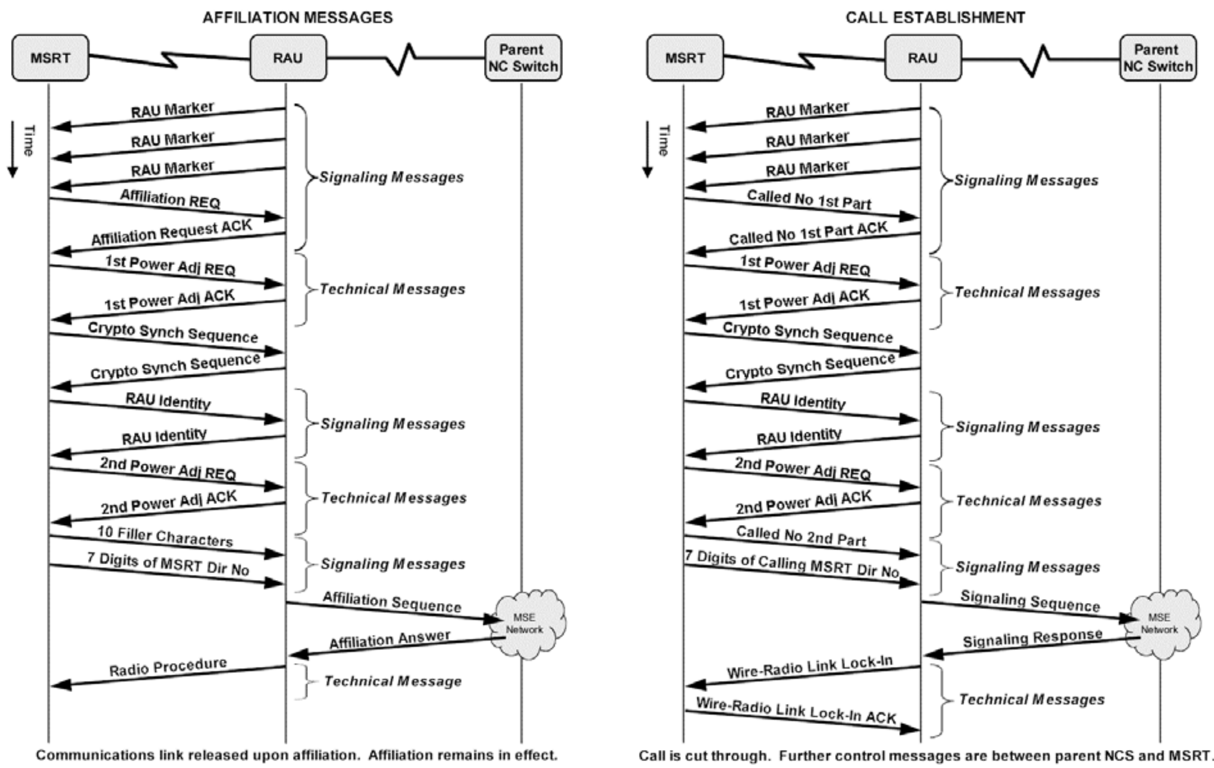


Figure 3. Control Messages Between the MSRT and RAU

Referenced materials did not indicate a named protocol for providing control. Systems requirements documents, SR13a, Part I [8] and SR13C, Part II [9], discuss Control Plane interactions for signaling control and supervision between the MSRT to the RAU. Section 5.2 introduces these procedures as the “General Dynamics Control Protocol.” [d]

Affiliation and call placement processes lay within Layers 2 and 3 of the Control Plane. The Data Link Layer attempts to make the physical link reliable and provides the means to activate, maintain, and deactivate the link. The principal service provided by the data link layer to higher layers is that of error detection and control [10]. Layer 2 affiliation of the MSRT involves interactions between the MSRT, RAU, and parent NCS. The process is similar to the three-way handshake used by the Transport Control Protocol (TCP) to establish an Internet data connection, but is more complex, because it includes the establishment of both a physical link

---

[d] Many of the protocols/procedures used in MSE are proprietary and were not given specific names in the reference material. Where appropriate, the authors assigned them names to simplify the discussion.

and a logical link. The process in the RAU/MSRT interface provides the capability to transfer data between an MSRT and its parent NCS, the switch where the Pre-Affiliation List (PAL) is stored. The PAL contains not only the telephone numbers to be used in the network, but also the unique capabilities and privileges given to individual numbers.

As noted above, interactions occur at several levels of the OSI model to make the passage of these messages possible. The Control Plane Individual End System Component Functionality Model given in Figure 4 serves as a reference in the following discussion of control message types and communications processes.

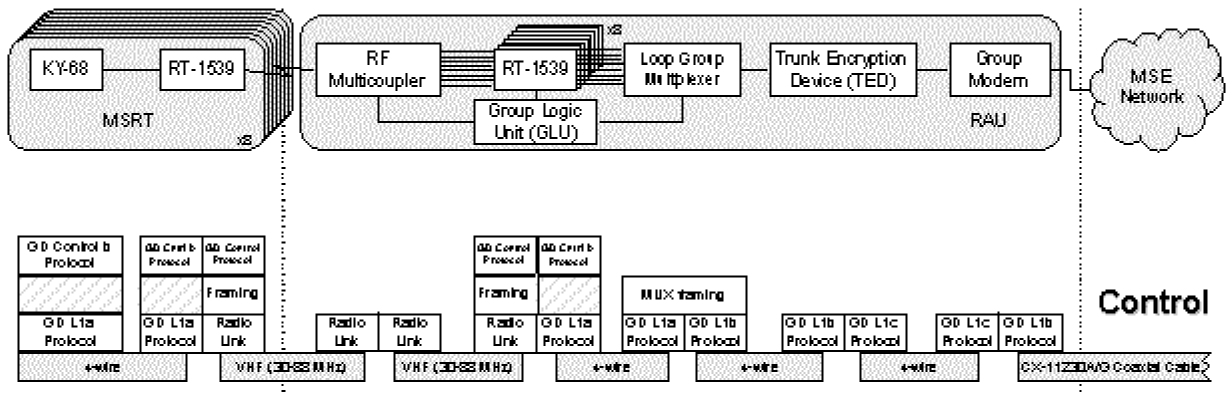
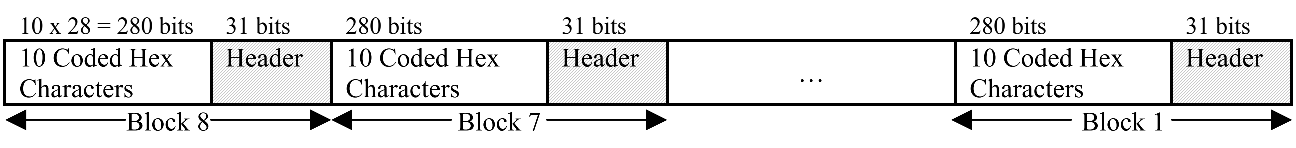


Figure 4. Control Plane Individual End System Component Functionality Model

5.2. General Dynamics Control Protocol Group

MSE exchanges control data in message form during all signaling sequences using two types of messages. Signaling Control messages (Figure 5) request and grant service, while Technical Control messages (Figure 6) provide engineering data that allow end and intermediate devices to provide service [11].

Signaling control messages are 2,488 bits long, and consist of eight blocks of ten characters each. Each block consists of a 31-bit header followed by 10 coded hexadecimal characters. Complementary 31-bit pseudo-random sequences define two different headers,



<u>Affiliation Messages</u>
Affiliation Request
Calling Number

<u>Absent Subscriber Features</u>
Disaffiliation Request
Calling Number

<u>Call Placement</u>
Called Number 1st Part
Called Number 2nd Part
Calling Number

<u>RAU</u>
RAU Marker

Figure 5. Signaling Control Messages and Message Format

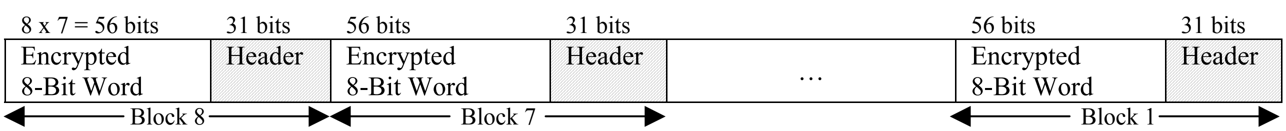
respectively called Header + (H+) and Header – (H-).   The receive-only controller decodes each block by performing several successive correlations. The first correlation, performed on 31 bits allows the controller to decode the header and, therefore, to be in-frame. The following correlations, performed on 31 bits provide for the decoding of each character within a block. The blocks are organized in order to allow the receive–only controller to perform a majority vote as required to improve the probability of right decoding in presence of extremely high bit error rates (up to 10%), likely to happen on VHF radio links. There are four types of Signaling Control Messages: Affiliation, Absent Subscriber, Call Placement, and RAU.

At Layer 1, the Physical Layer, Technical Control Messages consist of eight blocks of 87 bits each. Each block is obtained by coding each bit of an 8-bit word by a 7-bit pseudo-random sequence, and adding to the resulting 56 bits a 31-bit header. The 8-bit words are chosen so as to ensure that the distance between two words is always greater than or equal to four. Therefore, the length of a technical control message is always 696 bits. The most significant bit (MSB) is transmitted first. The receive-only controller decodes each block by performing several successive correlations, as previously described for signaling control messages. The blocks have an internal redundancy allowing them to be likely to happen on VHF radio links. There are five types of technical control messages: Affiliation, Link Establishment, Automatic Power Adjustment, Call Release, and Absent Subscriber.

5.3. Affiliation

The mobile subscriber affiliation process provides the capability for mobile subscribers to automatically affiliate at Layer 2. Once an MSRT affiliates with its parent node center switch—the one with the preaffiliation list (PAL) loaded—it is capable of placing calls within the MSE network. PALs [12] identify subscribers likely to affiliate with the network, define the unique subscriber numbers, and assign class of service profiles to each customer.

In order to affiliate, an MSRT must have the proper keys and frequency plan loaded, as



Affiliation Messages

8D—Affil. Request Granted, Radio Precedence Level, P

8E—Affil. Request Granted, Radio Precedence Level, R

5C—Wrong Personal Code Dialed

Affiliation Messages

C5—Subscriber Found on Black List

17—Subscriber Not Found or Request Not Accepted for Another Reason

Call Release Messages

17—Call Release

Link Establishment Messages

3A—Wire-Radio Link Lock-In

8E—Radio-Radio Link Lock-In

Absent Subscriber Feature Messages

8E—Request Accepted

17—Request Not Accepted (For Any Reason)

Automatic Power Adjustment Messages

E8—Transmit Full (N0) Power (16 W)

71—Transmit Medium (N1) Power (3 W)

A3—Transmit Low (N2) Power (0.5 W)

Figure 6. Technical Control Messages and Message Format

discussed in Section 7. The affiliation process begins when the subscriber dials the affiliation prefix (8R), Personal Code (PC) and the Directory Number. The subscriber must then go on-hook, allowing the MSRT to automatically search for a RAU marker on all assigned channels, moving through the assigned frequency plan on a cyclic basis. Each RAU continuously transmits a unique marker, which allows all non-affiliated MSRTs to make an affiliation attempt and all MSRTs currently affiliated to monitor the continuity of communication. The Group Logic Unit (GLU) in the RAU designates which of the RT-1539s will transmit the marker.

In case of a conflict between two requests, the RAU does not acknowledge the received messages. Instead, the scan cycle of each MSRT is automatically and randomly restarted so as to avoid the same situation during the subsequent attempt. When there is no conflict, the RAU acknowledges the received message by returning the same message to the MSRT. This message carries the disaffiliation prefix, the subscriber's personal code, and an End-of-Dialing (EOD) digit. Also, before acknowledging the received message, the RAU stops transmitting for 12 milliseconds. This allows the MSRT to perform a carrier transmission interruption test, which is needed to avoid situations in which the MSRT would be within range of two RAUs, the second RAU being engaged in another communication on the same frequency, but with the two RAUs being out of range from one another.

As soon as an MSRT successfully affiliates with a RAU/NCS, it stores the identity of this RAU. This allows the MSRT in the active standby mode to continuously check that it remains within the area covered by the RAU. The system compensates for short losses of contact due to hilly terrains absences by performing a statistical analysis at the MSRT. If the MSRT decodes fewer than eight markers out of sixteen complete consecutive scan cycles, it initiates a reaffiliation attempt with another RAU.

When an affiliated subscriber moves out of the current RAU's footprint, the radio subscriber access subsystem automatically reaffiliates his phone with a new RAU, allowing subscribers to move throughout the whole Corps area without any loss of communication capability, as long as they fall within the footprint of a RAU. Note, however, that this does not apply to current telephone calls. If a subscriber moves out of the range of a RAU while making a call, the call is dropped, and the subscriber must redial the MSRT.

If a user knows he is moving out of a covered area or that he will not be able to accept calls for an extended period of time, he may use an absent subscriber feature to manually request to disaffiliate his MSRT. This disaffiliation process is nearly identical to the affiliation process. The MSRT automatically searches for the marker of the RAU with which he is currently affiliated on all assigned channels, on a cyclic basis. When it decodes this marker, the MSRT locks in the corresponding channel by returning a disaffiliation request signal message to the RAU.

If the dissaffiliation is accepted, the NCS sends to the RAU a specific character to indicate this result [13]. The RAU then returns a "Request Accepted" Technical control message to the MSRT. If the disaffiliation is refused, the RAU receives from the switch a specific character indicating this result as specified in SR-01, and returns a "Request Not Accepted" Technical control message to the MSRT. An absent mobile subscriber will not be able to place any call to the network, with the sole exception of a call to the switch call service attendant. However, a subscriber will be able to place direct MSRT to MSRT calls.

When a subscriber turns off his MSRT, the system generates an automatic disaffiliation request. The radio set requires up to 20 seconds to power down, allowing sufficient time to send a disaffiliation request. The radio does not stay on long enough to receive the result of the request. The MSRT does not immediately delete the stored personal code and directory Number when it is powered down. They are retained in memory, powered by an internal battery, in order to allow first an automatic disaffiliation request to be performed, but also to allow the subscriber to power his radio set and to automatically reaffiliate with the network. Turning the MSRT off and on again is a good way to force it to reaffiliate with a new RAU in the event that the current RAU does not provide good communications. Because signaling and technical messages can be successfully transmitted over a radio path with BER of 10% percent, it is possible to affiliate with a RAU even though the poor connection cannot support voice communications where a CVSD encoder is used.

5.4. Call Origination, Release, and Preemption

The call routing process begins when the mobile subscriber dials the call precedence digit, the special service feature code, when required, and up to 13 digits for the called subscriber number. If the call precedence is not received, it is assumed to be Routine Precedence. When the radio set has collected the dialed sequence, the MSRT automatically searches for the marker of the RAU with which he is currently affiliated on all assigned channels, on a cyclic basis. (In the case of a non-affiliated subscriber to the RAU service attendant, however, any RAU marker is accepted.) The MSRT then decodes the presaturation status of his parent RAU.

MSE assigns users the capability to request certain precedence levels based upon the profiles assigned them in the PAL. These precedence levels are Flash Override (FO), Flash (F), Immediate (I), Priority (P), and Routine (R). Between the MSRT and the RAU, however, there are only two precedence levels. FO, F, and I are grouped into the "Priority" category and all others are grouped as "Routine." When two or fewer transceivers are available for traffic at the RAU, the RAU is said to be "presaturated." A presaturated RAU denies access to all non-priority calls. This traffic restriction rarely remains in force for an extended period, because as soon as at least three transceivers become available for traffic, the presaturation indicator is deleted.

When it decodes the RAU marker and when the call is authorized, the MSRT locks in the corresponding channel by returning a signaling message carrying the first part of the called number to the RAU. In the case of a conflict between two MSRTs, the RAU does not acknowledge the received messages; the scan-cycle of each MSRT is then automatically and randomly restarted so as to avoid the same situation during the subsequent attempt. When there is no conflict, the RAU acknowledges the received message by returning the received message to the MSRT. Lastly, when the radio equipment at the RAU receives this message, it reports this situation to the GLU, which designates another equipment (if any are available) to transmit the RAU marker.

Automatic power adjustment and synchronization of the COMSEC devices are performed. Upon synchronization of the COMSEC devices, the MSRT sends back the RAU identity number decoded at the beginning of the process. Upon completion of the received RF signal level measurement, a second power adjustment procedure is performed.

The two following signaling messages (Called Number Second Part and Calling Number) are used by the MSRT to transmit the remainder of the subscriber-dialed sequence and the subscriber's own directory number. These messages are on-line encrypted. The RAU is then able to transfer to the NCS up to 24 digits of the general form: (P) + (XC) + 9YX + XXX +

XXXXXXX + R + LNXXXXX. The meaning of these digits is given in SR-02 [14]. They are transferred to the NCS in accordance with procedures described in SR-01.

When all the digits have been transferred to the NCS, the RAU sends a LOCK-IN (wire to mobile) Technical message to the MSRT. After the required acknowledgement, which locks-in the radio link, both the RAU and the MSRT cut through and the subscriber may hear the tones sent by the switch. The call is then routed in the wire network in accordance with procedures described in SR-04 [15].

A Radio Release Protocol from the MSRT to RAU is initiated when a mobile subscriber engaged in a communication goes on-hook and his terminal sends the RELEASE code word to the MSRT. Upon decoding of this codeword, the MSRT sends a "Call Release" technical message to the RAU. The MSRT may then complete the sequence by sending the RELEASE ACK codeword to the terminal. The RAU then releases the line to the NCS, if not already released.

A Radio Release Protocol from the RAU to MSRT is initiated when any subscriber engaged in a communication with a mobile subscriber goes on-hook first; the parent switch of the mobile subscriber sends the RELEASE-2 codeword to the RAU. The RAU then sends a "Call Release" technical message to the MSRT and releases the line to the NCS. Call Preemption may be made on all calls established between a mobile subscriber and another subscriber of the MSE network by the NCS in order to set-up a new call to the same mobile subscriber, or, in order to reuse a radio equipment at the RAU so as to set-up a new call requested by a subscriber of higher precedence. In both cases, the call in progress must be released prior to establishing a new call.

6. The User Protocol Plane

The user protocol plane describes the transfer of user data back and forth between the source and the destination. The over all goal of this block is that this transfer of data is transparent to the user [16]. In the case of the MSRT to the RAU, the user protocol plane performs the function of transferring voice or data from the source to the destination.

6.1. Overview

Figure 7 illustrates the transfer of data in the user protocol plane. A circuit is set-up by the control protocol plane and connection-oriented data transfer takes place. A Continuously Variable Slope Delta Modulation (CVSD) codec transforms voice into data. The data is

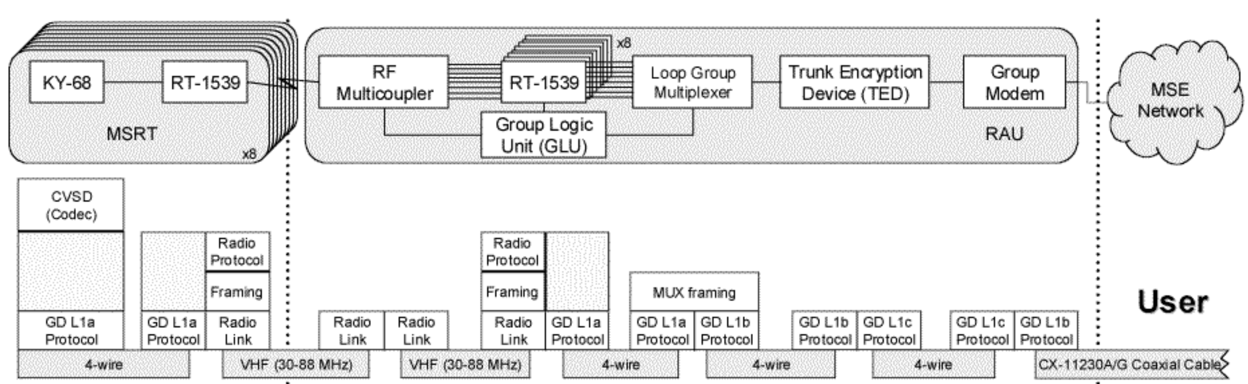


Figure 7. User Plane Individual End System Component Functionality Model

encoded, encapsulated, and then sent out into the MSE network as a bit stream. Understanding the handling of the bit stream at each significant device from the KY-68 through the RAU is key to understanding the system.

6.2. Continuously Variable Slope Delta Modulation Codec

Continuously Variable Slope Delta Modulation (CVSD) operates at the higher layers and converts the analog voice into a 16 kbps digital signal. CVSD compares the present voltage of a sample from a wave with the previous sample. If the present voltage is greater than the previous voltage, a "one" is output. If it is less, a "zero" is output. Each value of "one" steps up the slope of the digital signal while "zero" steps it down. CVSD does not provide as good of voice quality as many codecs, but it achieves understandable and recognizable voice with a low bit rate [17].

6.3. Radio Protocol

The Radio Protocol is a key piece to moving the data from the MSRT to the RAU. In the MSRT, this protocol takes the digital signal from the KY-68 and packetizes it at layer 3. This encapsulation is done in the RT-1539. At the RAU, decapsulation returns the data to its original state at the RT-1539.

The Radio Protocol packet consists of a 31-bit header, followed by 256 data bits, and ended with 20 or 21 filler bits (Figure 8). The purpose of these additional bits (51 or 52 total) is to change the bit rate from the terminal clock rate of 16 kbps to the radio clock rate of 19.2 kbps for transmission over VHF to the RAU. The one bit difference in filler bits is to correct the clock as 51 total bits results is a data rate of 19.1875 kbps and 52 total bits results in a data rate of 19.25 kbps. Under normal conditions one out of every five packets will contain 21 filler bits [18]. Once these bits are stripped off, the data rate once again assumes the terminal data rate of 16 kbps. Referenced materials do not indicate the specific contents of the 31-bit header. The filler bits are nothing more than bit stuffing.

20 or 21 Filler Bits	256 Data Bits	31 Header Bits

Figure 8. Radio Protocol Packet

6.4. General Dynamics Layer 1 Protocol Group

The General Dynamics Layer 1 (GD L1)[e] protocol group consist of GD L1a, GD L1b, and GD L1c. These protocols transport the bit stream from end system to end system from the KY-68 to out into the MSE network.

After the voice is converted to a digital signal in the KY-68 by the CVSD codec, the GD L1a protocol encodes the bit stream conditioned diphase (CDϕ) to eliminate the dc component and assist in maintaining timing. The bit stream gets transmitted from the KY-68 over a 4-wire medium to the RT-1539 [19]. The bit stream is encapsulated with the radio protocol (section 5.3)

[e] Many of the protocols/procedures used in MSE are proprietary and were not given specific names in the reference material. Where appropriate, the authors assigned them names to simplify the discussion.

and is transmitted at 19.2 kbps balanced conditioned diphase over radio frequency from antenna to antenna to the RAU.

Inside the RAU, the data is transmitted through many different components before being transmitted into the MSE network. Figure 1 illustrates the path the data takes from the MSRT, through the RAU, and into the MSE network.

The RF Multicoupler is the first device that handles the signal in the RAU. It has a diplexer, which permits parallel feeding into the omnidirectional antenna from multiple sources without interference [20]. The RF Multicoupler also contains a power divider, which transforms the signal received from the diplexer into separate 19.2 kbps signals to send to up to eight RT-1539s [21]. At the RT-1539, the signal is stripped of the additional bits added by the Radio Protocol (section 6.3) and converted back to a GD L1a bit stream.

Inside the Loop Group Multiplexer, the GD L1b protocol combines the eight conditioned diphase 16 kbps bit streams plus one 16kbps order wire into one conditioned diphase 256 kbps bit stream [22]. More is happening than simply combining these bit streams. There is also some layer two framing taking place. The referenced materials do not discuss this framing, however, it seems likely that this framing would utilize a portion of the additional 112 kbps difference after multiplexing the nine bit streams.

Inside the Trunk Encryption Device (discussed in more detail in section 7), the GD L1c protocol applies non-return to zero (NRZ) encoded data streams to the data producing a NRZ encoded 256 kbps signal [23]. The Group Modem applies the GDL1b protocol to convert the NRZ bit stream back into a balanced conditioned diphase 256 kbps bit stream for transmission over coaxial cable into the MSE network [24]. Table 1 summarizes the electrical characteristics of each of the above-mentioned interfaces.

	MSRT		**RAU**				
	KY-68 to RT-1539	RT-1539 to Multicoupler	Multicoupler to RT-1539	RT-1539 to LGM	LGM to TED	TED to GM	GM to NCS
Electrical Characteristics	3v pk-to-pk 16 kbps Conditioned Diphase Full duplex	High-16 W Med-3 W Low-0.5 W 19.2 kbps Conditioned Diphase Full duplex	3v pk-to-pk 19.2 kbps Conditioned Diphase Full duplex	3v pk-to-pk 16 kbps Conditioned Diphase Full duplex	3v pk-to-pk 256 kbps Conditioned Diphase Full duplex	3v pk-to-pk 256 kbps Non-return to Zero Full duplex	3v pk-to-pk 256 kbps Conditioned Diphase Full duplex

Table 1. Electrical Characteristics Between Wireless Components

7. The Security Protocol Plane

The Security Protocol Plane includes all measures taken to protect information from unauthorized access, use, or misuse. Security services are required to provide confidentiality, authentication, integrity, nonrepudiation, access control, and authentication to communications networks [25]. Security measures must also be taken to ensure the availability of the network services despite hostile actions to jam or disrupt them.

7.1. Overview

MSE secures its wireless communications with frequency plans, encryption, and signal strength management. Before an MSRT can be placed into operation, it must have a properly loaded frequency plan. The frequency plan assigns pairs of frequencies to be used for communication between the MSRT and the RAU. Cycling through these frequencies not only allows the system to handle multiple calls, but also provides an additional security measure, since users must know which frequency pairs to load in order to communicate. A variety of 128-bit communications security (COMSEC) keys encrypt all traffic, making the system suitable for traffic classified Secret and higher. Without the correct keys, an MSRT cannot affiliate with its parent node center, though non-secure calls to the operator are still possible. COMSEC keys secure individual network links as well as end-to-end connections. Finally, in order to reduce the probability of detection, the MSRT and RAU minimize transmission power to predetermined levels based upon the received strength of those signals. The security interactions necessary for affiliation and call placement are shown in Figure 9 and the Security Plane Individual End System Component Functionality Model given in Figure 10.

7.2. Frequency Plan

Communications between the MSRT and the RAU operate full duplex in the VHF frequency range (30-88 MHz). Network frequency plans may have up to 96 pairs of frequencies. MSRTs transmit on the low band in each pair, while RAUs transmit on the high band. Operators must load the plans by physically entering them using fill cables connected to another RT-1539 in an

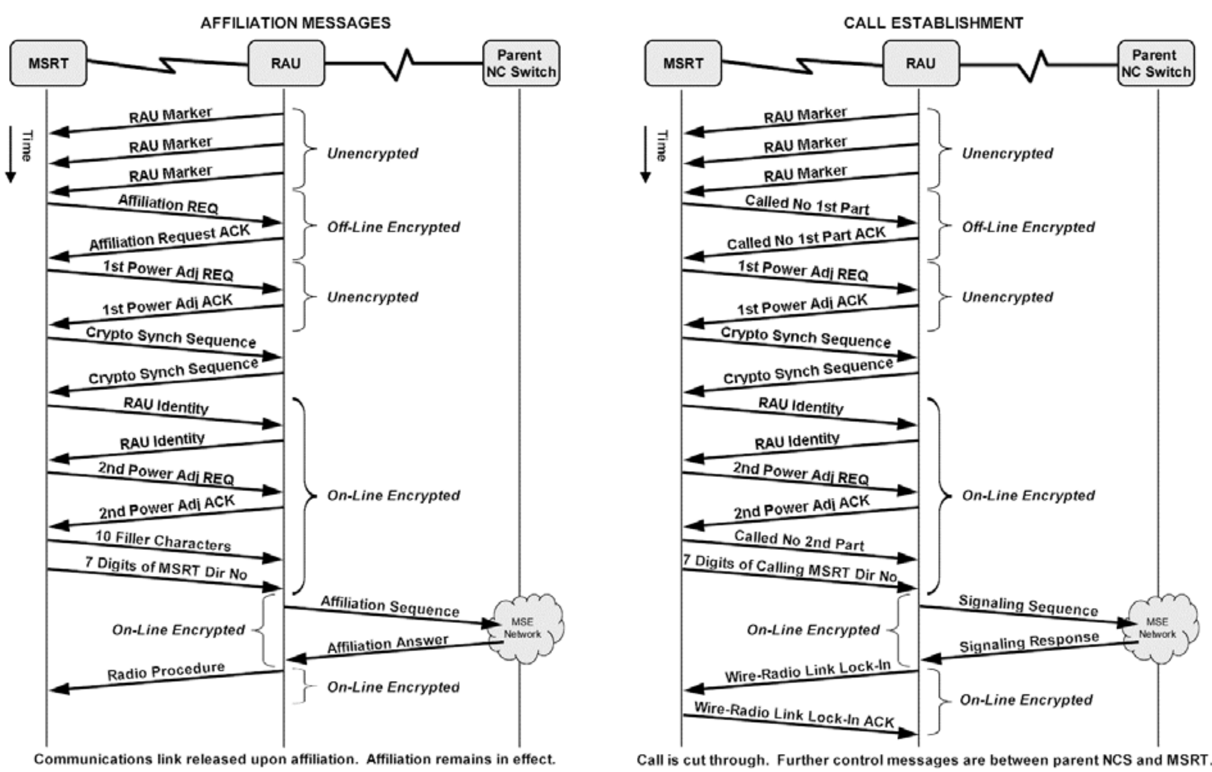


Figure 9. Security between the MSRT and the RAU

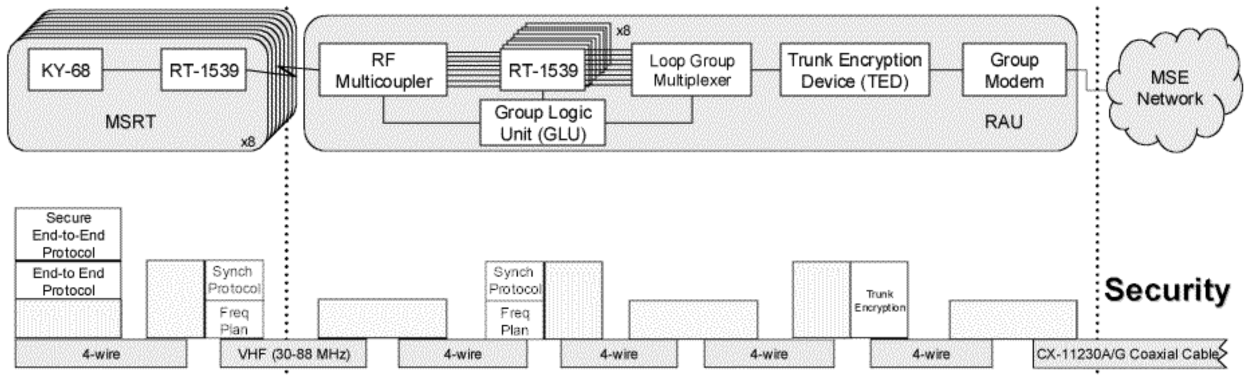


Figure 10. Security Plane Individual End System Component Functionality Model

MSRT or a RAU, or by manually entering them using the key pad on the DSVT. Users cannot gain access to the network unless they have a sufficient number of the correct frequency pairs loaded. Thus, frequency plans protect the network by denying access to those who do not have the proper frequencies and are unable to discover them.

As discussed in the control section, the RAU follows procedures to ensure that the frequencies used to set up individual calls are constantly changing, making it difficult for the enemy to target individual frequencies for jamming. MSRTs do not use frequency hopping or any other spread spectrum techniques once calls are established.

7.3. Encryption Protocol Group

MSE uses 128-bit Transmission Encryption Keys (TEKs) and Key Encryption Keys (KEKs). As their names suggest, TEKs encode transmissions whether they are individual calls or multiplexed signals, and KEKs are used to pass new keys to devices throughout the network. With respect to the MSRT and the RAU, there are five important types of keys as shown in Table 2. These keys

KEY	TYPE	EQUIPMENT	DISTRIBUTION	DESCRIPTION
M	TEK	DSVT KY-90 RT-1539 MCU	Corps Common	Re-entry/Initial entry. Signaling and synchronization between the MCUs in the RAU and MSRT.
V	TEK	DSVT KY-90	Unique Per Call	Unique per call associated with a DSVT/KY-90. Establishes end-to-end synchronization.
U1-U25	KEK	DSVT KY-90	One per subscriber determined by profile	Used to encrypt the V and X keys from the NCS/LENS to the terminal.
S	TEK	KY-68	Special Use	Generated and used by others to raise encryption level to TS/SCI (usually military intelligence (MI)).
X	TEK	DSVT KY-90	Corps Common	Encrypts calls associated with MSRT or DSVT users. Automatically replaces M key upon subscriber affiliation.

Table 2. COMSEC Keys Used With the MSRT and the RAU

operate at different locations and different encryption layers.

Encryption processes occur in DSVTs and in the Mobile COMSEC Units (MCU/MO-3(C)) contained in each of the RT-1539s. DSVTs operate as full-duplex voice and data terminals for 16 kbps or 32 kbps traffic. They provide the cryptographic functions, audio processing, and signaling necessary for secure and nonsecure access to switched networks, and secure point-to-point operation. MCUs are modules used to encrypt signaling between the MSRTs and the RAUs. Each MSRT RT-1539 has one MCU, while each RAU has eight, one for each of the eight RT-1539s in the RAU [26].

MSE uses both link encryption and end-to-end encryption. Link encryption establishes secure links between nodes in the MSE network, while end-to-end encryption secures the entire path between users. Encryption is performed between all links in the MSE network, whether they are between node centers, switches, or RAUs. End-to-end encryption, on the other hand, only encrypts paths between devices with encryption capability. For instance, if a DSVT is ultimately connected to a Digital Nonsecure Voice Terminal (DNVT), the SEN servicing the DNVT will serve as a proxy for securing the end-to-end encryption. Even though the wire between the SEN and the DNVT is not encrypted, the line is considered secure up to Secret, because the line is in a secure area. Figure 10 shows the layers of the encryption protocols and indicates where end-to-end and link encryption takes place. The diagram does not show the keys used at the trunk encryption device used for encrypting all circuits going to the node center, as they are beyond the scope of this paper.

The General Dynamics Link Encryption Protocol performs encryption at the lower protocol layers. With the General Dynamics Link Encryption Protocol, data is encrypted just before it is placed on the physical communication link. The process is invisible to the user. The link encryption protects the message in transit, and the message is in plaintext in intermediate equipment. It is especially vulnerable when a message must be passed through pieces of intermediate equipment, any of which may be untrusted. It is most appropriate when the transmission medium is the greatest point of vulnerability. Link encryption occurs within the MO-3(C)/G Mobile COMSEC Unit (MCU) of the RT-1539. Figure 10 identifies this particular instance of link encryption as a "synchronization protocol" which uses the same M key that is loaded into the DSVT for a different purpose, as discussed below.

The General Dynamics End-To-End Encryption Protocol performs encryption at the higher OSI layers. Data is in encrypted form throughout the network. The user is involved in the process, and the message is not in plaintext inside intermediate pieces of equipment. End-to-end encryption reduces vulnerability when a message is passed through several hosts, any of which may be untrusted. It is most appropriate when untrusted systems may be attached to the network. As shown in table 3, encryption can take place at several layers of the OSI Model [27]. Referenced documents do not indicate the precise layers where link and end-to-end encryption occurs, but it is likely that it occurs at Layer 2.

The RAU Marker is sent out unencrypted. During both the affiliation and call placement processes, the power adjustment signaling sequences are also unencrypted. Everything else has some form of encryption, unless the user chooses to go unsecure. When an MSRT is used to place a call, the signaling formats are off-line encrypted. Both the X and the M keys are used with the General Dynamics Link Encryption Protocol to establish Layer 2 encryption. To facilitate Layer 2 link encryption, the KY-68, the MSRT, and the RT-1539s in the RAU are manually coded with the M key. In order for the KY-68 to obtain initial re-entry and affiliation, it must have a correct M key. The M key is used with the General Dynamics Link Encryption

Open Systems Interconnection Layer	Responsibility	Description
Layer 7: Application	User Program	Initiates message; optional encryption
Layer 6: Presentation	System Utilities	Breaks message into blocks; text compression; optional encryption
Layer 5: Session	Operating System	Establishes user-to-user session, header added to show sender, receiver and sequencing information, recovery; optional encryption
Layer 4: Transport	Network Manager	Flow control, priority service, information added concerning the logical connection; optional encryption
Layer 3: Network	Network Manager	Routing, message blocking into packets, routing information added to blocks; optional encryption
Layer 2: Data Link	Hardware	Transmission error recovery, message separation into frames; optional encryption, header and trailer added for correct sequencing and error detection
Layer 1: Physical	Hardware	Physical signal transmission by individual bits

Table 3. Generalized Mapping of Encryption Within the OSI Model

Protocol to establish off-line Layer 2 encryption. Once the M key is verified and affiliation is granted by the switch the X key is generated by the KG-82 Loop Key Generator and the X key is sent from the switch, through the RAU, to the DSVT. The X key replaces the M key in the DSVT, and it provides on-line Layer 2 encryption.

The V key is used with the General Dynamics End-To-End Encryption Protocol to establish higher layer encryption during a call. To facilitate higher layer encryption, the V key is allowed to be passed to the KY-68 via the correct U key. Once the U key is authenticated, the switch sends the DSVT a per call V key generated by the KG-82 Loop Key Generator. As long as the call is from DSVT to DSVT, once the per call V key is distributed to both DSVTs, the switch drops the key, and only the two DSVTs have the V key. If the call is from a DSVT to a DNVT, then an intermediate switch has to hold the V key for the duration of the call. Use of the S key with the DSVT is another method of end-to-end encryption.

Once a call is encrypted from end to end, some users may opt to use another "secure end-to-end key" which is known only to them. This is the S key often employed by users discussing Top Secret (TS) and Special Compartmented Information (SCI). Only the end users have the key, because it is not generated by the KG-82 as are the other MSE keys.

Once the Wire-Radio Link Lock-In ACK is sent during the call process, the system is ready to send voice traffic, and the DSVT is using link encryption, end-to-end encryption, and possibly secure end-to-end encryption. Calls going out of the RAU and coming into the RAU from the rest of the MSE Network are encrypted and decrypted by a layer 1 KG-194 Trunk Encryption Device.

The format of the technical messages, signaling messages, and radio communications messages during Affiliation and Call Placement signaling messages are useful in showing the General Dynamics Encryption Protocol. The understanding of the format of the signaling messages, technical messages, and radio messages is important to the discussion of the layers at which encryption is occurring.

Pseudorandom numbers are used to code the technical messages and signaling messages. The M key and X key are used in conjunction with a General Dynamics Link Encryption Algorithm. When used with the synchronized COMSEC hardware, the General Dynamics Link Encryption Protocol performs a synchronized pseudorandom number selection and coding algorithm to encrypt information bits with 7 bit pseudorandom numbers. Signaling and technical message formats are shown below. A MSRT 10 character affiliation signaling message request is sent off-line encrypted to the RAU. Each one of the ten characters is a four bit binary representation of a hex character coded by 7 bit pseudorandom numbers for each bit, which yields 28 bits for each character. The RAU sends a 10-character affiliation signaling message acknowledge off-line encrypted as received to the MSRT. Note the three crypto context characters; these three characters are the means through which the MSE network verifies the M and U keys of the calling MSRT [28].

4 binary bits x 7 bit pseudorandom sequence = 28 bits per hexadecimal character 31 bits

Crypto Context	Crypto Context	Crypto Context	Data	Data	Data	Data	Data	Data	Data	Header
Character 10	9	8	7	6	5	4	3	2	1	

Figure 11. Individual Control Message Block.

The call placement signaling message also has three crypto context characters in characters eight through ten. The difference is that the characters 1 to 7 are up to the first 7 characters of the called number. The affiliation and the call placement messages are the only two signaling messages that have the 3 crypto context characters. Signaling messages are link encrypted off line with the M key or on line with the X key.

The coding of technical messages, shown in Figure 6, is the same as the coding of the signaling messages. Each bit of an eight bit word is coded by a 7 bit pseudo random sequence. Thus, one eight bit word is coded into (8 x 7 = 56) a 56 bit word, when coupled with the 31 bit header, forms an 87 bit block. Each technical message contains eight blocks for a total of 696 bits per technical message. Technical messages are also link encrypted off line with the M key or on line with the X key.

The actual voice traffic is sent using the radio communications message format, unless pre-empted or until the call is ended. The message format shown in figure 8 is link encrypted with the X key, and it is end-to-end encrypted using the per call V key. Once the call is established with the V key, it can be TS/SCI end-to-encrypted using the optional S key. Both the V key and the S key are used with the General Dynamics End-To-End Encryption Protocol. The radio message format is shown in figure 8.

7.4. Signal Strength Management

In order to minimize the RF power signature of the RAU and MSRTs, and thus, minimize the RF footprint seen by the enemy, the RAU and MSRT are designed to automatically reduce to the minimum power required. There are three possible RF levels delivered to the antenna: Full Power = N0 = 16W; Medium Power = N1 = 3W; and Low Power = N2 =.5W. The RAU automatically selects the lowest working output.

The affiliation and call placement processes begin at full RF power. However, when the first phase is completed, both the MSRT and the RAU attempt to reduce the RF power. Power is either maintained at full power or reduced to medium power, based upon the RF margin between the received signal and the receiver sensitivity. The corresponding indication is transmitted in the Automatic Power Adjustment Technical Message.

Simultaneous to the COMSEC synchronization, the RF signal level is measured again for about 2.2 seconds at both ends in order to adjust the transmitted power. Upon completion of the received RF signal level measurement, a second power adjustment procedure is performed. This time a power adjustment can be made to stay at the current level or go to the next higher or lower level among the three possible power levels.

8. The Management Function Plane

Communications systems, particularly those that pass a great deal of data, require sophisticated management tools to ensure that all subsystems are operating properly and that all users are receiving the service promised by those systems. There are five basic categories of management information. Sometimes referred to collectively as "FCAPS," these categories are Fault Management, Configuration and Name Management, Accounting Management, Performance Management, and Security Management. Most vendors of standardized and proprietary network management systems have adopted these standards [29].

8.1. Overview

The MSE Telecommunications Functional Model[f] proposed by a previous TSEC class covers in some detail how management is performed in MSE networks. Management takes place at Systems Control Centers, Node Center Switches, Large Extension Node Switches, and Small Extension Node Switches. MSE uses Integrated Management System (IMS) software as its application software. Over time, this software has improved to take advantage of many of the features offered by Simple Network Management Protocol (SNMP). Graphical user interfaces such as HP Openview facilitate network management. All of these tools operate primarily at the higher layers, making a layered model of management unnecessary.

8.2. Address Resolution

One of the most important functions of management is address resolution, a component of Configuration and Name Management. When a mobile subscriber affiliates his phone, he is asking the network to assign a certain number to his phone. The parent node center switch maintains a list of telephone numbers that are likely to be put into service. This Pre-Affiliation

[f] The Mobile Subscriber Equipment (MSE) Telecommunications Functional Model developed by students in a previous Telecommunications Systems Engineer Course (TSEC) class models the MSE network as a whole. The protocol reference model developed in this paper is much narrower in focus, concentrating only on the wireless components required for MSRT operations.

List (PAL) operates in the higher layers. Every time the MSRT places or receives a call, the parent NCS is involved. The PAL assigns all special capabilities to the affiliated telephone. The MSRT interacts with the parent NCS using the messages described in the control section. Thus, while management is involved in address resolution, from the standpoint of the MSRT and RAU these are simply control messages. The MSRT serves in a console capacity, sending messages necessary to interact with the PAL database.

8.3. Management Information Base

In March 1999, GTE Government Systems published an SNMP Management Information Base (MIB) Module defining and describing tactical circuit switches used in MSE and other tactical networks [30]. These definitions allow SNMP to set traps for and track important information about network health in both the circuit switched network and the packet switched network. They look at what is occurring at each switch in the network, but do not define RAUs or end user devices. The referenced MSE MIB module indicates that most management focuses on measuring the health of the network by looking at switches. There was little or no support for RAUs, and there was no support whatsoever for end user devices of any kind.

Still, network managers can learn a great deal about the health of the wireless network by viewing reports generated at the switches. They can tell when a number attempts to affiliate, when it places a call, or when it is dropped, because every action an end user makes requires the telephone to be affiliated with its parent node center, where the PAL is stored.

9. Conclusions

The MSRT to RAU Protocol Reference Model provided in this paper is, by no means complete. Just as volumes have been written to describe what happens at each of the layers of the OSI model, one would expect that the MSRT to RAU Protocol Reference Model would similarly result in more detailed documents explaining specific aspects of key protocols and layers. For instance, the 31-bit header used in control messages and radio messages, the algorithms used to encrypt traffic using 128-bit keys, and the possible development of MIBs to manage end-user devices are all worthy of additional investigation. The importance of the protocol reference model presented in this paper is that it establishes the solid framework required for precisely this kind of study, development, and application.

9.1. Insights into MSE's Treatment of Unique Military Requirements

The MSRT to RAU Protocol Reference Model certainly does provide some key insights into how this wireless component of the MSE system addresses the unique military requirements of low probability of detection (LPD), resistance to jamming, precedence and perishability, interoperability with legacy systems, security, and electromagnetic compatibility.

As discussed in the control and security section of the paper, MSE adjusts transmission power to one of three levels depending upon measured receive levels. This capability, already important from an engineering standpoint, also benefits the end user by reducing the probability of detection. One of the big drawbacks to any wireless telephone system is the requirement for sending out constant beacons. In MSE, these beacons are a liability for both the RAU and the MSRT, but the ability to reduce power once a connection is made helps to reduce the threat of detection. However, this ability is relatively unimpressive when compared to the capability of modern cellular systems to constantly adjust power levels across a more continuous range.

While these protocols require the addition of overhead, they may be worthy of consideration for insertion into the RT-1539.

The MSRT to RAU framework also includes certain provisions for reducing jamming. As described in the control section, RT-1539s employ frequency plans of up to 96 sets of frequencies. The use of multiple frequency sets, used on a per call basis, makes hostile jamming of MSRT calls challenging at best. Network engineers reduce friendly jamming by placing RAUs in a manner that minimizes mutual interference. In the event that one MSRT attempts to affiliate with multiple RAUs, the system directs how to release the redundant links. One of the greatest anti-jamming capabilities of the wireless system is its rapid entry into the backbone system, where highly directional LOS radios continue to move the signal. Thus, an MSRT user in a forward position can communicate with anyone in the MSE network without trying to increase his transmission power and making himself a target for jamming or artillery.

The control section identifies how the wireless system addresses precedence and perishability. MSE subscribers may be assigned one of four precedence levels depending upon the profile identified on the PAL, but precedence means nothing if those users can't access the network. The ability of a RAU to drop a user in order to allow another user access to the network is essential to ensuring that key users can pass information before it is too late. Many proposed wireless solutions do not provide the same degree of service to subscribers based upon their authorized and requested precedence levels.

The RAU makes the circuit switched network available to wireless subscribers through a number of ingenious methods. The Radio Protocol, discussed in the user plane section, is essential to the merging of the switched network with the wireless network. Before the military procured new equipment to replace any switch, access unit, or end user device, it should ensure that access is provided as efficiently. Relying on a pure commercial solution might result in reduced capabilities, particularly when viewed in conjunction with precedence and perishability concerns.

The MSE network derives all of its security form 128-bit keys used for transmission of traffic and encryption of other keys. Four of the eighteen basic types of keys required for the entire network are specifically for establishing communications between wireless subscribers and the network. These keys guarantee all users the certainty that they are communicating on a secret high system. Additional S keys allow users to use unique end-to-end encryption. The use of the 128-bit key for all MSE encryption may be an interoperability concern for some commercial systems being considered for integration into the legacy or future systems. Certainly, any other type of key would create an additional key management burden.

Finally, the physical layer considerations discussed in the Control section are especially important to evaluating potential wireless systems for military use. MSRTs use frequencies that are clearly within the military spectrum, making, at the very worst, a subset of them available for use in any theater of operation. VHF has another advantage over most cellular systems—range. RT-1539s operate at a nominal range greater than that of most cellular systems.

9.2. Recommendations

The usefulness of the protocol reference model in evaluating unique requirements of military communications systems is indicative of its usefulness as an Army Signal Corps standard. In researching the paper, the authors discovered that the ability to describe system processes in terms of the OSI model gave them credibility, a common ground for discussing complex ideas, and a framework for explaining the interrelated ideas of user, control, security, and management principles. When dealing with engineers, discussions of signaling, control, and radio messages naturally led to questions involving what occurred at the physical, data link, network, and higher layers. Unfortunately, the product specifications and engineering documents did not follow any layered approach to MSE communications. This is not surprising because today's industry standard models were not available when MSE was developed.

Obviously, the laws of physics have not changed, and the techniques used in developing MSE are just as valid whether they are presented in accordance with a layered protocol reference model. Never the less, the time has come to evaluate all communications systems from a common reference point. Army signal personnel should learn about MSE and future systems in terms of common models. Their ability to understand systems in terms of industry models will help them to take advantage of the convergence of military and commercial technologies, understand legacy systems and identify strategies for upgrading or replacing them, and, perhaps most importantly, teach them the language of telecommunications.

The MSRT to RAU Protocol Reference Model demonstrates the effectiveness of applying current industry telecommunications models to understand legacy communications systems. These models provided a framework for identifying key pieces of the system's architecture, and established a foundation for further study. The model helped to identify strengths and weaknesses of the existing communications system, and suggested logical points to insert new technology. Finally, it demonstrated that the use of familiar models makes it possible to learn about any unfamiliar system very quickly. Technology changes more rapidly each year, but simple models allow telecommunications engineers, professionals, and end users to efficiently assess key features, capabilities, and weaknesses. These models are invaluable in keeping up with legacy, current, and future communications systems.

Citations

[1] Eric Blair, Bryon Hartzog, Mark Mattei, Reggie Morgan, and Hubert Wagstaff, "The Mobile Subscriber Equipment (MSE) Telecommunications Functional Model," thesis, Fort Gordon, Sep. 2001.

[2] Philip M. Feldman, *Emerging Commercial Mobile Wireless Technology and Standards: Suitable for the Army?* (Santa Monica: RAND Press, 1998) 6-8.

[3] HQ, Dept of the Army, TM 11-5800-216-10-1, *Mobile Subscriber Equipment System Manual* (Sep. 1991).

[4] Office of the Project Manager, *Warfighter Information Network*, website (Fort Monmouth, 8 Dec. 2001) <http://www.monmouth.army.mil/peoc3s/win-t/main/msefrme.htm>.

[5] Feldman, 14-19.

[6] ITU-T, ITU-T Recommendation I.320, *ISDN Protocol Reference Model,* (Nov. 1993) 5.

[7] Philip Enslow Jr., *Understanding Telecommunications Systems*, 12th ed. (Atlanta: Georgia Institute of Technology, Sep. 2000).

[8] GTE Government Systems Corporation, Mobile Subscriber Division, Taunton, MA, SR 13A, Part I, *Configuration Item Nomenclature RAU/MSRT Interface Control Documents Functional Interface Description*, Specification Date, 6 Mar. 1987

[9] GTE Government Systems Corporation, Mobile Subscriber Division, Taunton, MA., SR 13C, Part II, *Configuration Item Nomenclature RAU/MSRT Interface Control Documents Operational Interface Description*, Specification Date, 15 Oct. 1991

[10] William Stallings, *Data & Communications*, 6th ed. (New Jersey; Prentice Hall, 2000) 52.

[11] GTE Government Systems Corporation, Mobile Subscriber Division, Taunton, MA., SR 05H, *Mobile Subscriber Signaling Plan*, Specification Date, 17 Feb. 1993

[12] HQ, Dept of the Army, FM 11-38, *MSE System Management and Control* (Apr. 1991) ch. 2.

[13] GTE Government Systems Corporation, Mobile Subscriber Division, Taunton, MA., SR 01, *NCS/RAU Interface Control Document*, Specification Date, 17 Feb. 93.

[14] GTE Government Systems Corporation, Mobile Subscriber Division, Taunton, MA., SR 02, *Numbering Plan*, Specification Date, 17 Feb. 93.

[15] GTE Government Systems Corporation, Mobile Subscriber Division, Taunton, MA., SR 04, *Network Signaling Diagrams*, Specification Date, 17 Feb. 93.

[16] I.320, 5.

[17] Enslow, 2-23.

[18] GTE Government Systems Corporation, Mobile Subscriber Division, Taunton, MA., SR 13A, Part I, *Configuration Item Nomenclature RAU/MSRT Interface Control Documents Functional Interface Description*, Specification Date, 6 Mar. 1987, 12.

[19] HQ Dept of the Army, TM 11-5820-1021-23&P, *Terminal, Radio-Telephone, Mobile Subscriber: AN/VRC-97* (Sep. 1991) 4-1.

[20] Harry Newton, *Newton's Telecom Dictionary,* 17th ed. (New York: CMP Books, Feb. 2001) 211.

[21] HQ Dept of the Army, TM 11-5820-1022-13-1, *Radio Access Unit: AN/TRC-191A* (Feb. 1996) 6-6.

[22] Ibid, 1-7.

[23] Ibid, 6-9.

[24] Ibid, 1-7, 6-11.

[25] William Stallings, *Cryptology and Network Security*, (Upper Saddle River: Prentice Hall, 1999) 4-5.

[26] Chairman of the Joint Chiefs of Staff, C2 Systems Directorate (J-6), CJCSM 6231, *Manual for Employing Joint Tactical Communications* CD-ROM (Oct. 200 1) app. F.

[27] Department of Computer Science, *Information Assurance*, security class notes (Naval Postgraduate School, 1994) < http://www.cs.nps.navy.mil/curricula/tracks/security/notes/chap10_9.html#HEADING8>.

[28]Chairman of the Joint Chiefs of Staff, C2 Systems Directorate (J-6), CJCSM 6231, *Manual for Employing Joint Tactical Communications* CD-ROM (Oct. 200 1) ch. 2

[29] William Stallings, *SNMP, SNMPv2, SNMPv3 and RMON 1 and 2*, 3rd ed. (Boston: Addison-Wesley, 1999) ch. 1.

[30] GTE Government Systems Corporation, Communications Systems Division, Taunton, MA, *GTEGSC2Circuit Switch Common REGTC Definitions*, Last Updated Jun 1999.